

UNITED STATES DISTRICT COURT

for the
District of MassachusettsIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Room 7341 of Pine Dale Hall at the University of
Massachusetts at Dartmouth

Case No.

H.J. # 13-2104-MBB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

Room 7341 of Pine Dale Hall at the University of Massachusetts at Dartmouth as further described in Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before May 3, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m.☒ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Marianne B. Bowler

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

4/21/13 @ 12:14
04/20/2013 0:00 am AMMarianne B. Bowler
Judge's signature

City and state: Brookline, Massachusetts

Marianne B. Bowler, U.S. Magistrate Judge

Printed name and title

DT-0000162

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

<i>Return</i>		
<i>Case No.:</i>	<i>Date and time warrant executed:</i>	<i>Copy of warrant and inventory left with:</i>
<i>Inventory made in the presence of :</i>		
<i>Inventory of the property taken and name of any person(s) seized:</i>		
<i>Certification</i>		
<p><i>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</i></p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p><i>Date:</i> _____</p> </div> <div style="width: 60%;"> <p style="text-align: center;">_____ <i>Executing officer's signature</i></p> <p style="text-align: center;">_____ <i>Printed name and title</i></p> </div> </div>		

DT-0000163

ATTACHMENT A

PREMISES TO BE SEARCHED

The location to be searched is **Room 7341 of Pine Dale Hall** (“the Target Residence”), at the University of Massachusetts at Dartmouth, located at 285 Old Westport Road, North Dartmouth, Massachusetts. Pine Dale Hall is a student residence located on the campus of the University of Massachusetts at Dartmouth. Pine Dale Hall is a four-story brown building, which contains 208 double rooms and is equipped with two elevators for student use. The words “Pine Dale Hall” is written in black letters above the doorway.

The front door to Room 7341 does not have a number on its door. The front door is a wooden door which is emblazoned with several stickers that read “Dzhokhar 7341” and his roommate’s name followed by “7341.”

ATTACHMENT B

ITEMS TO BE SEIZED

All evidence inside the premises and curtilage located at the Target Residence, related to violations of 18 U.S.C. §§ 2332(a) (Using and Conspiring to Use A Weapon of Mass Destruction), 844(i) (Malicious Destruction of Property by Means of an Explosive Device Resulting in Death), and 371 (Conspiracy to Commit Offenses), including but not limited to:

1. Property, records, items, or other information, related to violations of the aforementioned statutes, including but not limited to, bomb making material and equipment, explosive material, components of bomb delivery devices;
2. Property, records, or other information related to the ordering, purchasing, manufacturing, storage, and transportation of explosives;
3. Property, records, or other information related to the ordering and purchasing of pressure cooker devices, BBs, nails, and other small metallic objects;
4. Property, records, or information related to the Boston Marathon;
5. Property, records, or information related to any plans to initiate or carry out any other attacks inside or outside the United States, or any records or information related to any past attacks;
6. Property, records, or information related to the state of mind and/or motive of Tamerlan and Dzhokhar to undertake the Boston Marathon bombings;
7. Property, records, or other information related to the identity of Tamerlan and Dzhokhar;
8. Property, records, or other information related to the identity of any individuals who were in contact with, or were associates of Tamerlan and Dzhokhar;
9. Property, records, or information, related to any organization, entity, or individual in any way affiliated with Tamerlan and Dzhokhar, that might have been involved in planning, encouraging, promoting the actions described herein;
10. Property, records, or other information, related to Tamerlan's and/or Dzhokhar's schedule of travel or travel documents;
11. Property, records, or information related to any bank records, checks, credit card bills, account information, and other financial records.

12. Personal property, including articles of clothing, consistent with the appearance of Tamerlan and Dzhokhar as seen in surveillance video on April 15, 2013, as described above.

13. All digital evidence, as that term is used herein, means the following:

A. Any computer equipment or digital devices that are capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, including central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices such as modems, routers, cables, and connections; storage media; and security devices;

B. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes referenced above, or to create, access, process, or store evidence, contraband, fruits, or instrumentalities of such crimes;

C. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes;

D. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

E. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

F. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

G. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

H. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital

device, that show the actual user(s) of the computers or digital devices during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

DIGITAL EVIDENCE SEARCH PROCEDURE

In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

(A) On-site search, if practicable. Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on-site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

(B) On-site imaging, if practicable. If a digital device cannot be searched on-site as described above, the computer personnel, if present, will determine whether the device can be imaged on-site in a reasonable amount of time without jeopardizing the ability to preserve the data.

(C) Seizure of digital devices for off-site imaging and search. If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

(D) Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

(E) Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law


enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

(F) If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

(G) If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

(H) If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return		
Case No.: M.J. # 13-2104-MBB	Date and time warrant executed: 04/21/2013, 2:43 a.m.	Copy of warrant and inventory left with: INSIDE ROOM 7341, PINE DALE HALL.
Inventory made in the presence of: CAPTAIN TIMOTHY M. SHEEHAN, UMASS DARTMOUTH POLICE DEPARTMENT.		
Inventory of the property taken and name of any person(s) seized: PLEASE SEE COPY OF PROPERTY RECEIPT ATTACHED HERETO.		
Certification		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date: 08/21/2013	 Executing officer's signature JOHN WALKER, SA, FBI, BOSTON Printed name and title	

DT-0000169